PRIVACY IMPACT ASSESSMENT (PIA)

For the

Wounded Warrior Accountability System (WWAS)
Department of the Army - US Army Medical Command

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐ **New DoD Information System** ☐ **New Electronic Collection**

☒ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒ **Yes, DITPR** Enter DITPR System Identification Number: 5191 (DA76900)

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:

☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI 007-21-01-03-02-1399-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier A0040-66b DASG

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 1071-1085, Medical and Dental Care; 50 U.S.C. Supplement IV, Appendix 454, as amended, Persons liable for training and service; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b TRICARE Prime and TRICARE Program; 10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, CHAMPUS; 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; E.O. 9397, as amended (SSN); DoD Instruction 6015.23, Delivery of Health care at Military Treatment Facilities (MTFs); DoD Directive 6040.37, Confidentiality of Medical Quality Assurance (QA) Records; DoD 6010.8-R, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); Army Regulation 40-66, Medical Record Administration and Health Care Documentation.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

WWAS is an Army Chief of Staff initiative that is vital in providing services and programs to assist Army Wounded Warriors (AW2). WWAS currently supports AW2, Ombudsman (OMB), and the Wounded Solider Family Hotline (WSFH) Programs. WWAS provides data and process infrastructure as well as the integrated applications that support the accurate, timely and effective tracking and management of Warfighters in the Wounded Warrior Lifecycle. The data, process infrastructure, and integrated applications support Wounded Warriors in various stages of medical treatment/rehabilitation, medical evaluation, physical disability evaluation, and physical disability compensation.

The types of personal information collected includes military, demographic/personal, employment, educational, and medical information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with the PII collected are unauthorized access, inaccurate information entered into the application, and unauthorized disclosure of PII. Security safeguards are in place to mitigate these risks.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Data is shared with Warrior Transition Program personnel in all MEDCOM organizations.

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. Data is shared with the AW2 advocates within Veterans Affairs.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. 1. The following is the contract language for all Information Technology Support Order (ITSO) contractors:

H.8 SECURITY REQUIREMENTS

The contractor performing work under this Task order shall be cleared in accordance with the procedures set forth in AR 25-2, AR 525-13, and Directives of the Command Information Program. While no present requirement for classified work has been identified, individual subtasks and projects may include a requirement for Contractor staff clearances up to and including TOP SECRET. At a minimum, all contractor personnel performing work under this Task Order are required to have a completed National Agency Check (NAC).

The DD Form 254 is applicable to this requirement and is provided in Section J, Attachment D. The contractor and all subcontractors must possess the required security clearance, based on job requirements, prior to performing functions on the TO. The contractor and all subcontractors must maintain the required security clearance throughout the life of the task order. Only U.S. citizens shall be used to perform work under the requirements of this TO. The contractor shall provide security clearance information to the HRC Security and Information Assurance Offices.

HRC is heterogeneous, enterprise-operating environment consisting of servers, network devices, workstations, printers and other peripherals. Contractors must have Information Assurance certification training commensurate with the level of work they perform. The Contractor is responsible for ensuring all its employees possess all the required licenses or certificates necessary in the execution of this TO. Systems Administrators (SA) and Network Administrators (NA) must be designed IT-I, IT-II or IT-III. Each SA or NA must be trained, experienced, IA certified and currently certified on the information system they are required to maintain. The SA and NA must hold a U.S. Government Secret security clearance and local access approval commensurate with the level of information processed on the system or network. All Contractor SA and NA personnel must possess, at minimum a Secret or Interim Secret clearance. The Contractor is required to be familiar with all systems, platforms and languages contained in Infrastructure Inventories.

Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552A and applicable agency rules and regulations.

2. The following contract language pertains to the Wounded Soldier Family Hotline (WSFH) contractors. The contractor for WSFH is National Sourcing Incorporate:

1.6.7 Security Requirements: The contractor shall be responsible for obtaining all necessary security clearances such as National Agency Check (Trustworthy) required by applicable guidelines, regulations and directives that are necessary to provide contractor personnel access to an installation's network backbone. Provisions of the privacy act apply to all records and reports maintained by the contractor. Contractor personnel may be required to obtain and maintain installation security badges, Common Access Cards, AKO Accounts and to adhere to security requirements of installations. Contractor personnel will control unclassified documents that require For Official Use Only (FOUO) document designation. If a DD 254 is required, the unit security monitor will initiate a DD 254 that will become an attachment to this PWS.

3. The following contract language pertains to the Army wounded Warrior (AW2) contractors. The contract of AW2 is Serco:

16.0. SECURITY REQUIREMENTS. The contractor is responsible for safeguarding information of a confidential or sensitive nature. Failure to safeguard any classified/ privileged information which may involve the contractor or the contractor's personnel or to which they may have access may subject the contractor and/or the contractor's employees to criminal liability under Title 18, section 793 and 7908 of the United States Code. Provisions of the Privacy Act apply to all records and reports maintained by the contractor. All programs and materials developed at Government expense during the course of this contract are the property of the Government. Contractor personnel shall be required to obtain and maintain security badges, SECRET clearance and otherwise adhere to the installation security requirements. The performance of this requirement will require the contractor access to classified information. FAR clause 52-204-2, Security Requirements, as required by either FAR Subpart 4.404 (a) or FAR Subpart 4.404(d), whichever is appropriate. At the time that the solicitation is issued, it shall be accompanied by a Contract Security Specification, DD Form 254, in accordance with DoD Directive 5220.22-M, Department of Defense Industrial Security Manual for Safeguarding Classified Information, and any revisions, thereto, as well as Industrial Security Regulation DoD 5220.22-R. Failure to safeguard and classified/privileged information that may involve the contractor and/or the contractor's personnel, or to which they may have access, may subject the contractor and/or contractor's personnel to criminal liability under Title 18, section 793 and 7908 of the United States Code. Provisions of the Privacy Act apply to all records and reports maintained by the contractor. Contract personnel shall maintain and possess a valid SECRET security clearance for access to classified information. Currently, personnel supporting USSOCOM at Walter Reed Army Medical Center and Fort Bragg will require a TOP SECRET clearance and this may occur at other sites.

4. The following contract language pertains to the Ombudsman (OMB) contractors. The contract for OMB is Eagle Applied Sciences:

(a) The Contractor shall not use or further disclose Protected Health Information other than as permitted or required by the Contract or as Required by Law.

(b) The Contractor shall use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Contract.

(c) The Contractor agrees to use administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits in the execution of this Contract.

(d) The Contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Health Information by the Contractor in violation of the requirements of this Clause. These mitigation actions will include as a minimum those listed in the TMA Breach Notification Standard Operating Procedure (SOP), which is available at: http://www.tricare.mil/tmaprivacy/breach.cfm.

(e) The Contractor shall report to the Government any security incident involving protected health information of which it becomes aware.

(f) The Contractor shall report to the Government any use or disclosure of the Protected Health Information not provided for by this Contract of which the Contractor becomes aware.

(g) The Contractor shall ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by the Contractor, on behalf of the Government, agrees to the same restrictions and conditions that apply through this Contract to the Contractor with respect to such information.

(h) The Contractor shall ensure that any agent, including a subcontractor, to whom it provides electronic Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect it.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals are verbally notified that furnishing any PII is voluntary; however, failure to provide information may result in a delay or error in processing and/or denial of being part of the Army Wounded Warrior Program.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

An intake form with a Privacy Act Statement is given to the soldier to authorize the disclosure of their information. The soldier signs the form at intake into the program.

(2) If "No," state the reason why individuals cannot give or withhold their consent.